DANIEL L. WARSHAW (SBN 185365)
dwarshaw@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, CA 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

MELISSA S. WEINER (*Pro Hac Vice* Forthcoming)
mweiner@pswlaw.com
JOSEPH C. BOURNE (SBN 308196)
jbourne@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

MADISON COPELAND, individually and on behalf of all others similarly situated, Plaintiff, v. [24]7.AI, INC., Defendant.	CASE NO. 5:18-CV-5859 **COMPLAINT** CLASS ACTION JURY TRIAL DEMANDED

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Plaintiff Madison Copeland, on behalf of himself and all others similarly situated, files this Class Action Complaint against Defendant [24]7.ai., Inc., based upon personal knowledge with respect to himself and on information and belief derived from the investigation of counsel and review of public documents as to all other matters, alleges as follows:

SUMMARY OF THE CASE

1. Plaintiff brings this class action against Defendant for its failure to secure and safeguard customers' payment card data ("PCD") and other personally identifiable information ("PII") that Defendant collected while Plaintiff and Class members shopped on Best Buy, Delta, or Sears's website or chatted with customer service on Best Buy, Delta, or Sears's website in the Fall of 2017. Plaintiff also brings this action against Defendant for its failure to provide timely, accurate, and adequate notice to Plaintiff and Class members that their PCD and PII (hereinafter, collectively, "Customer Data") had been compromised and stolen. Due to Defendant's introduction of security vulnerabilities to Best Buy, Delta, and Sears's websites and its failure to adequately secure Plaintiff and Class members' Customer Data, it was accessed by third parties without authorization by Plaintiff or Class members (the "Data Breach").

2. Defendant is a customer experience software and services company headquartered in San Jose, California, with approximately 12,000 employees. Defendant offers sales and service-oriented software, as well as voice and chat agent services, for sales and support. Best Buy, Delta, and Sears have used Defendant for such services since at least, and likely well before, September 27, 2017—the purported beginning of the Data Breach described herein.

3. Best Buy is a retail company with over 1,000 stores throughout the United States providing technology products, services, and solutions. Best Buy offers "expert service" more than 1.5 billion times every year to consumers, small business owners, and educators who visit and patronize Best Buy stores. Best Buy also provides the "Geek Squad" service to further facilitate its goal of providing technology products, services, and solutions. Best Buy markets and makes these products and services available through various distribution channels, including its website and over the phone.

4. Delta provides air transportation for passengers in the United States and abroad.

Delta sells tickets through various distribution channels including, among others, its website, mobile application, and over the phone.

5. Sears is a retail company with over 500 stores throughout the United States providing a large variety of products and services. Sears markets and makes its products and services available through various distribution channels, including its website and over the phone.

6. In the last few years, retailers such as Target, Home Depot, Kmart, Wendy's, Neiman Marcus, and Brooks Brothers have experienced streams of attacks on their data security. Implementing measures to prevent those attacks, as well as quickly identifying them, has become a normal, expected part of the business.

7. On April 4, 2018, Delta and Sears announced that they had suffered a data breach caused by data security failures relating to their use of Defendant's customer service chat services product.

8. On April 5, 2018, Best Buy acknowledged that customers who shopped online or used Best Buy's outsourced chat services for customer support were also potential victims of the Data Breach and their Customer Data was stolen.

9. This private Customer Data was compromised due to Defendant's acts and omissions and its failure to properly protect the Customer Data that became compromised through consumers' use of the Best Buy website and the security vulnerabilities that Defendant introduced to Best Buy's website.

10. Defendant could have prevented this Data Breach. Data breaches in the last few years have been the result of infiltration of computer systems in which Customer Data is exchanged. While many retailers, restaurant chains, and other companies using such systems have responded to recent breaches by adopting technology that helps make communication and transactions more secure, Defendant did not.

11. In addition to Defendant's failures to prevent the Data Breach, Defendant also failed to disclose the Data Breach for approximately six months, despite detecting and allegedly

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

remedying the breach on October 12, 2017.[1]

12. The Data Breach was the inevitable result of Defendant's inadequate approach to data security and the protection of the Customer Data that it collected during the course of their business.

13. Defendant acknowledges that it collects personal information, including: first and last names; organization names; email addresses; phone numbers; physical addresses; dates of birth; gender; professional title; account information; credit/debit card numbers; and other information Defendant needs to provide client-specified services.[2] Indeed, Defendant claims to follow "industry standards to protect the security of End Users' Personal Information and Defendant respects End Users' choices for such information's intended use."[3] Defendant allegedly uses "a combination of reasonable and appropriate physical, technical, and administrative safeguards to prevent unauthorized access or disclosure of End Users' Personal Information," and that it "retains Personal Information and Interaction Data only as required or permitted by local law and while it has a legitimate business purpose."[4] Finally, Defendant represents that it "uses standard security protocols, and mechanisms to exchange the transmission of sensitive Personal Information such as credit card details and login credentials."[5]

14. Best Buy, Delta, and Sears have all also recognized that their customers entrust them with their personal information, which Best Buy, Delta, and Sears and their partners and agents—such as Defendant—have an obligation to safeguard.[6]

---

[1] *Id.*

[2] [24]7.ai, Inc., Platform Privacy Policy, *available at:* https://www.247.ai/privacy-policy#platform-policy (last visited August 20, 2018).

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] Best Buy Code of Business Ethics, Privacy Policy, *available at:* https://secure.ethicspoint.com/domain/media/en/gui/26171/code.html?section=7&sub=4 (last visited August 20, 2018); Delta, Cookies, Privacy & Security, *available at:* https://www.delta.com/content/www/en_US/privacy-and-security.html (last visited April 30, 2018); Sears, Privacy Policy, *available at*: https://www.sears.com/en_us/customer-service/policies/privacy-policy.html (last visited Sept. 13, 2018).

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

15. Unfortunately, Defendant did not meet its security promises.

16. Instead, Defendant disregarded the rights of Plaintiff and Class members by failing to take adequate and reasonable measures to ensure its data systems were protected, failing to disclose to its customers the material fact that they did not have adequate computer systems and security practices to safeguard Customer Data, failing to take available steps to prevent and stop the Data Breach from ever happening, failing to timely monitor and detect the Data Breach, and failing to timely notify consumers of the Data Breach.

17. In addition, Defendant, which was an agent of Best Buy, Delta, and Sears, caused and exacerbated the damages Plaintiff and Class members suffered by failing to timely detect the infiltration and failing to timely notify customers their Customer Data had been compromised. If Defendant had detected the malware earlier and promptly notified Best Buy, Delta, Sears, and the public of the Data Breach, the resulting losses would have been far less significant.

18. As a result of the Data Breach, the Customer Data of Plaintiff and Class members has been exposed to criminals for misuse—the very reason this information was taken. As discussed in more detail below, the damages Plaintiff and Class members suffered as a direct result of the Data Breach include unauthorized charges on their debit or credit cards, theft of their personal and financial information, costs associated with the detection and prevention of identity theft, loss of access to their account funds and associated costs, the time spent addressing these issues, and money paid for Best Buy purchases that they otherwise would not have spent.

19. The damages to Plaintiff and Class members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for Customer Data.

20. The damages to Plaintiff and Class members were also directly and proximately caused by Defendant's failure to inform them that their Customer Data was subject to collection and storage by Defendant.

21. Plaintiff retains a significant interest in ensuring that his Customer Data, which remains in the possession of Defendant, is protected from further breaches. Accordingly, he seeks to remedy the harms he has suffered on behalf of himself and other similarly situated consumers

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

whose Customer Data was stolen as a result of the Data Breach.

22. Plaintiff, on behalf of himself and other similarly situated consumers, seek to recover damages, equitable relief (including injunctive relief to prevent a reoccurrence of the Data Breach and resulting injury), restitution, disgorgement, reasonable costs and attorneys' fees, and all other remedies this Court deems proper.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendant.

24. This Court has personal jurisdiction over Defendant because Defendant is headquartered in this District, conducts substantial business in this District, and committed the acts and omissions complained of in the District.

25. Venue is proper under 28 U.S.C. § 1391(c) because Defendant's principal place of business is in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions that that led to the Data Breach.

INTRADISTRICT ASSIGNMENT

26. This action arises in Santa Clara County, where Defendant is headquartered and where the relevant decisions and actions giving rise to the Data Breach occurred. Pursuant to Local Civil Rule 3-2(e), this action shall be assigned to the San Jose Division.

PARTIES

27. Plaintiff Madison Copeland is a resident of the State of Alabama.

28. Defendant [24]7.ai is a California corporation that performs customer service functions for retailers and companies alike. Defendant's principal place of business and corporate headquarters is located in San Jose, California.

FACTUAL BACKGROUND

A. Plaintiff's Transactions

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

29. Plaintiff regularly makes purchases at Best Buy and other online retailers. For his purchases, he uses a credit card.

30. Between September 19, 2017, and October 17, 2017, Plaintiff made five purchases online through Best Buy's website, www.bestbuy.com. These purchases included a purchase on October 6, 2017, of computer and printer equipment and supplies.

31. On May 1, 2017, Plaintiff received a letter from Best Buy, which was titled "NOTICE OF DATA BREACH" and dated April 25, 2018 (the "Notice Letter").

32. The Notice Letter advised Plaintiff that "we have determined that your personal information may have been affected by this incident." Best Buy blamed "malicious code that was inserted in" Defendant's software, which is used to provide Best Buy's customer service chat function. This allowed "an unauthorized party to access payment information of certain Best Buy customers who shopped on BestBuy.com" between September 26, 2017, and October 12, 2017. This information "included cardholder names, addresses and payment card information (including payment card number, expiration date and security code)." Best Buy claimed that it and Defendant had undertaken steps to try to fix the security flaws that had led to the data breach.

33. After reviewing the Notice Letter, Plaintiff spent approximately four hours researching the Data Breach and the security of his payment card information. Plaintiff works as a self-employed information technology contractor and bills his time at a rate of $50 per hour.

34. Plaintiff would not have used his payment card to make online purchases of merchandise from Best Buy had Defendant and Best Buy told him they lacked adequate computer systems and data security practices to safeguard customers' Customer Data from theft. Thus, he was injured by paying money for purchases of merchandise from Best Buy that he would not have made had Defendant disclosed to him the vulnerabilities it introduced on the Best Buy website.

35. Plaintiff suffered injury from having his Customer Data compromised and stolen in the Data Breach.

36. Plaintiff also suffered injury in the form of damages to and diminution in the value of his Customer Data—a form of intangible property that he entrusted to Defendant through his

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

use of the Best Buy website employing Defendant's technology, and which was compromised as a result of the Data Breach.

37. Plaintiff further suffered injury in the form of time spent dealing with the Data Breach.

38. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Customer Data being placed in the hands of criminals.

39. Moreover, Plaintiff has a continuing interest in ensuring that his private information, which remains in the possession of Defendant and Best Buy, is protected and safeguarded from future breaches.

B. Defendant Collects and Stores Customer Data for Its Own Financial Gain

40. Founded in 2000,[7] Defendant operates a variety of customer services products with artificial intelligence technologies with additional offices in Toronto, London, Stockholm, and Sydney, and numerous clients in retail, education, financial services, healthcare, insurance, travel and hospitality, and utilities.[8]

41. Since its founding, Defendant has aggressively expanded, including private funding from Sequoia Capital—a venture capital firm controlling $1.4 trillion in assets—in 2003, as well as a partnership with Microsoft in 2012, in which Microsoft combined its "interactive self-service assets" with Defendant's technologies.[9]

42. At all relevant times, Defendant was aware, or reasonably should have been aware, that the Customer Data collected, maintained, and stored in Defendant's computer systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties,

---

[7] [24]7.ai Company Profile, Forbes, https://www.forbes.com/companies/24-7/ (last visited April 30, 2018);

[8] [24]7.ai Company Overview, https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=4532786 (last visited April 30, 2018)

[9] *Microsoft picks stake in Sequoia-backed [24]7.ai Inc*, Reuters, https://in.reuters.com/article/microsoft-picks-stake-in-sequoia-backed-idINDEE81807U20120209 (last visited May 1, 2018)

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

such as identity theft and fraud.

43. It is well known and the subject of many media reports that Customer Data is highly coveted and a frequent target of hackers. Despite the frequent public announcements of data breaches by other retailers, Defendant maintained an insufficient and inadequate system to protect Plaintiff's and Class members' Customer Data.

44. Customer Data is a valuable commodity because it contains not only payment card numbers but PII as well. A "cyber blackmarket" exists in which criminals openly post stolen payment card numbers, and other personal information on the internet, including the dark web. Customer Data is valuable to identity thieves because they can use victims' personal data to open new financial accounts and take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

45. Legitimate organizations and the criminal underground alike recognize the value in PII contained in a merchant's data systems; otherwise, they would not aggressively seek or pay for it. For example, in "one of 2013's largest breaches . . . not only did hackers compromise the [card holder data] of three million customers, they also took registration data [containing PII] from 38 million users."[10]

46. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Customer Data and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on consumers as a result of a data breach.

47. Defendant was, or reasonably should have been, fully aware of the significant volume of daily credit and debit card transactions and PII provided in customer service interactions and purchases and, thus, the significant number of individuals who would be harmed by a breach of Defendant's systems.

---

[10] Verizon 2014 PCI Compliance Report, available at: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf (hereafter "2014 Verizon Report"), at 54 (last visited April 30, 2018).

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

48. Despite all of this publicly available knowledge of the continued compromises of Customer Data in the hands of other third parties, such as retailers, Defendant's approach to maintaining the privacy and security Plaintiff's and Class members' Customer Data was inadequate and unreasonable.

C. Defendant Had Notice of Data Breaches Involving Malware on POS Systems

49. A wave of data breaches causing the theft of retail payment card information has hit the United States in the last several years.[11] In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a 40% increase in the number of data breaches from the previous year.[12] The amount of payment card data compromised by data breaches is massive. For example, it is estimated that over 100 million cards were compromised in 2013 and 2014.[13]

50. Many of the data breaches occurring within the last several years involved malware placed on computer systems that retail merchants and their agents use.

51. These data breaches involve compromising payment systems at physical retail outlets, phishing schemes to gain access to internal servers and information, and exploiting other vulnerabilities in companies' websites and electronically stored data systems.

D. The Data Breach

52. On April 4, 2018, Delta and Sears announced that that the Data Breach had compromised their customers' information. The Customer Data was stolen as a result of security vulnerabilities introduced by the companies' use of Defendant's software and technology.

53. Best Buy announced the Data Breach on April 5, 2018. According to its statements, Best Buy was informed of the Data Breach on March 28, 2018. The Customer Data was stolen as

---

[11] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, Identity Theft Resource Center (Jan. 19, 2017), http://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208 (last visited April 13, 2018).

[12] *Id.*

[13] Symantec, *A Special Report On Attacks On Point-of-Sale Systems*, p. 3 (Nov. 20, 2014), available at: https://origin-www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf (last visited April 13, 2018).

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

a result of security vulnerabilities introduced by the companies' use of Defendant's software and technology.

54. Defendant possibly knew of the Data Breach as early as September 26, 2017, and definitively on October 12, 2017, when Defendant allegedly fixed the security issues.[14]

55. Despite knowing of the Data Breach since at least October 12, 2017, Defendant has not provided any details regarding the degree and extent of the Data Breach—even though it handles chat services for Best Buy, Delta, Sears, and several other large companies.

E. The Data Breach Caused Harm and Will Result in Additional Fraud

56. Without detailed disclosure of the nature and scope of the Data Breach, consumers, including Plaintiff and the Class, have been left exposed—unknowingly and unwittingly—for six months to continued misuse, and ongoing risk of misuse, of their Customer Data without being able to take necessary precautions to prevent imminent harm.

57. The ramifications of Defendant's failure to keep Plaintiff's and Class members' Costumer Data secure are severe.

58. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[15] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[16]

59. PII is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[17]

---

[14] *Updates on [24]7.ai Cyber Incident: Statement from [24]7.ai*, https://www.bestbuy.com/site/privacy-policy/247-ai-cyber-incident/pcmcat1522954594900.c?id=pcmcat1522954594900 (last visited August 20, 2018).

[15] 17 C.F.R § 248.201 (2013).

[16] *Id.*

[17] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited April 13,

(footnote continued)

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

60. Identity thieves can use personal information to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

61. Identity thieves have stolen $112 billion in the past six years.[18]

62. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the DOJ found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[19]

63. There may be a time lag between when harm occurs and when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

64. Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class members are incurring and will continue to incur such damages in addition to any fraudulent credit and debit

---

2018).

[18] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited April 13, 2018).

[19] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited April 13, 2018).

[20] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited April 13, 2018).

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

card charges incurred by them and the resulting loss of use of their credit and access to funds, whether or not such charges are ultimately reimbursed by the credit card companies.

F. Plaintiff and Class Members Suffered Damages

65. Plaintiff's and Class members' Customer Data is private and sensitive in nature, and Defendant left that Customer Data inadequately protected and caused it to be inadequately protected. Defendant did not obtain Plaintiff's and Class members' consent to disclose their Customer Data to any other person, as required by applicable law and industry standards.

66. The Data Breach was a direct and proximate result of Defendant's failure to properly safeguard and protect Plaintiff's and Class members' Customer Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law. These failures include Defendant's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Customer Data to protect against reasonably foreseeable threats to the security or integrity of such information.

67. Defendant had the resources to prevent a breach. For example, Defendant is funded by Sequoia Capital and partners with Microsoft.

68. Had Defendant employed security measures recommended by experts in the field, Defendant would have prevented intrusion into their computer systems and, ultimately, the theft of their customers' Customer Data.

69. As a direct and proximate result of Defendant's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud. This increased risk requires Plaintiff and Class members to take the time (which they otherwise could have dedicated to other life demands, such as work or personal endeavors) and effort to mitigate the actual and potential impact of the Data Breach, including by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

recaptured. In all manners of life in this country, time has constantly been recognized as compensable; for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a retailer's negligent or unlawful conduct, as is the case here.

70. Defendant's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' Customer Data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Customer Data being placed in the hands of criminals;

d. the improper disclosure of their Customer Data;

e. loss of privacy;

f. the monetary amount of purchases at Best Buy, Delta, or Sears during the period of the Data Breach that Plaintiff and Class members would not have made had they known adequate systems and procedures to reasonably protect their Customer Data were absent;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. ascertainable losses in the form of deprivation of the value of their Customer Data, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and

k. the loss of productivity and value of their time spent to attempt to address the actual and future consequences of the Data Breach, including finding fraudulent charges; canceling and reissuing cards; purchasing credit monitoring and identity theft protection services; imposition of withdrawal and purchase limits on compromised accounts; and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

71. Defendant has not offered credit monitoring or identity theft protection services to any affected customers directly. Even retailers have not offered *adequate* credit monitoring or identity theft protection services. For instance, Best Buy has stated that it will offer credit monitoring or identity theft protection services limited to one year, even though criminals can and often do simply sit on the stolen Customer Data for more than one year and then misuse it. As a result, Plaintiff and Class members are left to their own actions to adequately protect themselves from the financial damage Defendant has allowed to occur. The additional cost of adequate and appropriate coverage, or insurance, against the losses and exposure that Defendant's actions have created for Plaintiff and Class members is ascertainable and is a determination appropriate for the trier of fact.

72. While Plaintiff's and Class members' Customer Data has been stolen, Defendant continues to hold Customer Data of consumers, including Plaintiff and Class members. Because Defendant has demonstrated an inability to prevent a breach or promptly stop it, Plaintiff and Class members have an undeniable interest in ensuring that their Customer Data is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CHOICE OF LAW

73. Defendant is incorporated and headquartered in San Jose, California. That is the nerve center of Defendant's business activities—the place where high-level officers direct, control, and coordinate Defendant's activities, including data security, and where: (a) major

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

policy; (b) advertising; (c) distribution; (d) accounts receivable departments; and (e) financial and legal decisions originate.

74. Data security assessments and other IT duties related to computer systems and data security occur at Defendant's California headquarters. Furthermore, Defendant's response, and corporate decisions surrounding such response, to the Data Breach were made from and in California. Finally, Defendant's breach of its duty to customers—including Plaintiff and Class members—emanated from California.

75. It is appropriate to apply California law extraterritorially to the claims against Defendant in this case due to Defendant's significant contacts with California. Defendant is headquartered in California; the relevant decisions, actions, and omissions were made in California; and Defendant cannot claim to be surprised by application of California law to regulate its conduct emanating from California.

76. To the extent California law conflicts with the law of any other state that could apply to Plaintiff's claims against Defendant, application of California law would lead to the most predictable result, promote the maintenance of interstate order, simplify the judicial task, and advance the forum's governmental interest.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

CLASS ACTION ALLEGATIONS

77. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure, Plaintiff brings this lawsuit on behalf of himself and on behalf of the proposed nationwide class (the "Class") defined as follows:

> All persons who use Defendant's electronic customer service platform or who shopped on Best Buy, Delta, or Sears's website or mobile application, and whose Customer Data was compromised as a result of the Data Breach.

78. Excluded from the Class are Defendant and any entities in which Defendant or its subsidiaries or affiliates have a controlling interest; Defendant's officers, agents, and employees; and all persons who make a timely election to be excluded from the Class. Also excluded from the Class are the judge assigned to this action, and any member of the judge's immediate family.

79. **Numerosity:** The members of the Class are so numerous that joinder of all Class members would be impracticable. Plaintiff reasonably believes that Class members number in the hundreds of thousands of people or more in the aggregate. The names and addresses of Class members are identifiable through documents Defendant and third parties (such as Delta, Best Buy, and Sears) maintain.

80. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

i. Whether Defendant owed a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, and safeguarding their Customer Data;

ii. Whether Defendant breached a legal duty to Plaintiff and Class members to exercise due care in collecting, storing, and safeguarding their Customer Data;

iii. Whether Defendant knew or should have known of the susceptibility of its computer systems to a data breach;

iv. Whether Defendant knew or should have known of the susceptibility it cased in Delta, Best Buy, and Sears's computer systems to a data breach;

v. Whether Defendant's security measures to protect its computer systems were reasonable in light of industry data security standards and recommendations;

vi. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and Class members' Customer Data;

vii. Whether Plaintiff's and Class members' Customer Data was accessed, exposed, compromised, or stolen in the Data Breach;

viii. Whether Defendant was negligent in failing to implement reasonable and adequate security procedures and practices;

ix. Whether Defendant's failure to implement adequate data security measures allowed the breach of their computer systems to occur;

x. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the loss of Plaintiff's and Class members' Customer Data;

xi. Whether Defendant failed to timely notify the public of the Data Breach;

xii. Whether Defendant's conduct constituted deceptive trade practices;

xiii. Whether Defendant's conduct violated California's Unfair Competition Law;

xiv. Whether Defendant's conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*;

xv. Whether Plaintiff and Class members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

xvi. Whether Plaintiff and Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief, and the amount thereof.

81. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

82. **Typicality:** Plaintiff's claims are typical of Class members' claims because, among other things, Plaintiff and Class members were injured through Defendant's substantially uniform misconduct. Plaintiff are advancing the same claims and legal theories on behalf of themselves and Class members, and there are no defenses that are unique to Plaintiff's claims. Plaintiff's and Class members' claims arise from the same operative facts and are based on the same legal theories.

83. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class members he seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation, including data privacy and data security practices litigation; and Plaintiff will prosecute this action vigorously for the benefits of the Class. Class members' interests will be fairly and adequately protected by Plaintiff and his counsel.

84. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

85. Further, Defendant has acted or refused to act on grounds generally applicable to Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

86. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to, the elements of Plaintiff and Class members' claims and Defendant's liability.

CLAIMS ALLEGED ON BEHALF OF THE CLASS

First Claim for Relief

Negligence

87. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in the above numbered paragraphs as though fully stated herein.

88. Upon accepting and storing Plaintiff's and Class members' Customer Data in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Customer Data was private and confidential and should be protected as private and confidential.

89. Defendant owed a duty of care not to subject Plaintiff and Class members, along with their Customer Data, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

90. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their Customer Data and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure Plaintiff's and Class members' Customer Data was adequately secured and protected. Defendant further had a duty to implement processes that would detect a breach of their data system in a timely manner.

91. Defendant knew that Plaintiff's and Class members' Customer Data was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if Plaintiff's and Class members' Customer Data was

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

wrongfully disclosed, that disclosure was not fixed, or Plaintiff and Class members were not told about the disclosure in a timely manner.

92. By being entrusted by Plaintiff and Class members to safeguard their respective Customer Data, Defendant had special relationships with Plaintiff and Class members. Plaintiff and Class members made purchases through Best Buy, Delta, or Sears's website and/or utilized Defendant's customer service chat product with the understanding that Defendant would take appropriate measures to protect their Customer Data and would inform Plaintiff and Class members of any breaches or other security concerns that might call for action. But Defendant did not. Defendant not only knew its data security was inadequate, it also knew it did not have the tools to detect and document intrusions or exfiltration of Customer Data. Defendant is morally culpable, given its wholly inadequate safeguards, as well as their refusal to notify Plaintiff and Class members of breaches or security vulnerabilities.

93. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' Customer Data by failing to adopt, implement, and maintain adequate security measures to safeguard that information, and allowing unauthorized access to Plaintiff's and Class members' Customer Data.

94. Defendant also breached its duty to timely disclose that Plaintiff's and Class members' Customer Data had been, or was reasonably believed to have been, stolen, exposed, or compromised.

95. Defendant's failure to comply with industry standards further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' Customer Data.

96. But for Defendant's respective wrongful and negligent breach of its duty owed to Plaintiff and Class members, their Customer Data would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's respective negligence was a direct and legal cause of the theft of Plaintiff's and Class members' Customer Data, as well as the resulting damages.

97. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

Plaintiff's and Class members' Customer Data. Defendant knew its computer systems and technologies for accepting and securing Plaintiff's and Class members' Customer Data had numerous security vulnerabilities.

98. As a result of Defendant's misconduct, Plaintiff's and Class members' Customer Data was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Customer Data was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their Customer Data in that it is now easily available to hackers on the dark web. Plaintiff and Class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Second Claim for Relief

Negligence *Per Se*

99. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in the above numbered paragraphs as though fully stated herein.

100. Section 5(a) of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Customer Data.

101. Defendant violated Section 5(a) of the FTC Act by failing to use reasonable measures to protect Customer Data and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Customer Data they obtained and stored, and the foreseeable consequences of the Data Breach, including, the damages that would result to Plaintiff and Class members.

102. Defendant's violation of Section 5(a) of the FTC Act constitutes negligence *per se*.

103. Plaintiff and Class members are within the class of persons the FTC Act was intended to protect.

104. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses,

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that Plaintiff and Class members suffered.

105. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered, and continue to suffer, injuries and damages. Such damages arise from and include Plaintiff's and Class members' inability to use their debit or credit cards because those cards were canceled, suspended, or otherwise rendered unusable as a result of the Data Breach; false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged and foregone cash back rewards; lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports; and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

Third Claim for Relief

Violation of California's Unfair Competition Law

(Cal. Bus. & Prof. Code § 17200, *et seq.*)

106. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in the above numbered paragraphs as though fully stated herein.

107. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200 *et seq.*

108. Defendant stored the Customer Data of Plaintiff and Class members in its computer systems. Defendant falsely represented to Plaintiff and Class members that their Customer Data was secure and would remain private.

109. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

have kept Plaintiff's and Class members' Customer Data secure and prevented the loss or misuse of that Customer Data.

110. Even without these misrepresentations, Plaintiff and Class members were entitled to assume, and did assume, that Defendant would take appropriate measures to keep their Customer Data safe. Defendant did not disclose at any time that Plaintiff's Customer Data was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

A. Unlawful Business Practices

111. As noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, both by affirmative conduct and by omission, the safety of its computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and Class members' Customer Data.

112. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security, failing to comply with its own posted privacy policies, and by failing to immediately notify Plaintiff and Class members of the Data Breach.

113. If Defendant had complied with these legal requirements, Plaintiff and Class members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiff and Class members of the Data Breach.

114. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the FTC Act.

115. Plaintiff and Class members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In particular, Class members have suffered from fraudulent charges to their credit/debit card accounts as a result of the Data Breach. In addition, Plaintiff and Class members' Customer Data was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class members have also suffered consequential out

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

B. Unfair Business Practices

116. **Defendant engaged in unfair business practices under the "balancing test."** The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and misrepresentations to consumers about Defendant's data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff and Class members, directly causing the harms alleged below.

117. **Defendant engaged in unfair business practices under the "tethering test."** Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

118. **Defendant engaged in unfair business practices under the "FTC test."** The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects hundreds of thousands of Class members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and Class members' Customer Data to third parties without their consent, diminution in value of their Customer Data, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiff's and Class members' Customer Data remains in Defendant's possession, without adequate protection, and is also in the hands of those

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

who obtained it without their consent. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. *See* 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g., In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

119. Plaintiff and Class members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. In particular, Class members have suffered from improper or fraudulent charges to their credit/debit card accounts; and other similar harm, all as a result of the Data Breach. In addition, Plaintiff and Class members' Customer Data was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

120. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiff and Class members are entitled to injunctive relief and reasonable attorneys' fees and costs.

Fourth Claim for Relief

Unjust Enrichment

121. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in the above numbered paragraphs as though fully stated herein.

122. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, Plaintiff and Class members patronized Best Buy, Delta, and Sears and provided them with their payment information and provided Defendant with their Customer Data. In exchange, Plaintiff and Class members should have been entitled to have Defendant protect their Customer Data with adequate data security.

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

123. Defendant has received compensation from Best Buy, Delta, and Sears for providing them the products and services that resulted in the Data Breach.

124. Defendant knew that Plaintiff and Class members conferred those benefits, and Defendant accepted or retained that benefit. Defendant profited from the purchases and used Plaintiff's and Class members' Customer Data for business purposes.

125. Defendant failed to secure Plaintiff's and Class members' Customer Data and, therefore, did not provide full compensation for the benefit Plaintiff and Class members provided.

126. Defendant acquired the Customer Data through inequitable means and failed to disclose the inadequate security practices previously alleged.

127. If Plaintiff and Class members knew that Defendant would not secure their Customer Data using adequate security, they would not have transacted with Best Buy, Delta, or Sears via their website or mobile application or used the online chat feature, or otherwise provided their Customer Data to Defendant.

128. Plaintiff and Class members have no adequate remedy at law.

129. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred.

130. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that Defendant unjustly received.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of Class members, respectfully requests that this Court enter an Order:

a. Certifying Class, and appointing Plaintiff and his Counsel to represent Class;

b. Finding that Defendant's conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

c. Enjoining Defendant from engaging in further negligent, deceptive, unfair, and unlawful business practices as alleged herein;

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

d. Awarding Plaintiff and Class members actual, compensatory, consequential, and/or nominal damages;

e. Awarding Plaintiff and Class members statutory damages and penalties, as allowed by law;

f. Requiring Defendant to provide appropriate credit monitoring services to Plaintiff and Class members;

g. Compelling Defendant to use appropriate cyber security methods and policies with respect to data collection, storage, and protection, and to disclose with specificity to Class members the type of Customer Data compromised;

h. Awarding Plaintiff and Class members pre-judgment and post-judgment interest;

i. Awarding Plaintiff and Class members reasonable attorneys' fees, costs and expenses, and;

j. Granting such other relief as the Court deems just and proper.

DATED: September 24, 2018

PEARSON, SIMON & WARSHAW, LLP

By: */s/ Daniel L. Warshaw*
DANIEL L. WARSHAW

DANIEL L. WARSHAW (SBN 185365)
dwarshaw@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, CA 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

MELISSA S. WEINER (*Pro hac vice* forthcoming)
mweiner@pswlaw.com
JOSEPH C. BOURNE (SBN 308196)
jbourne@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, MN 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610

Attorneys for Plaintiff and the Proposed Class

PEARSON, SIMON & WARSHAW, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403